NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2810.1A
Effective Date: May 16, 2006
Expiration Date: May 16, 2011

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Security of Information Technology

Responsible Office: Office of the Chief Information Officer

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

SECTION IV OPERATIONAL CONTROLS

a. Once the requirements for a system have been defined, other factors must be considered to ensure the security of that system. Operational controls are controls that are implemented and executed by people, as opposed to systems. These controls are implemented to improve the security of a particular system or group of systems. They often require technical or specialized expertise and often rely upon management activities, as well as technical controls.

b. Requirements for operational controls include personnel and user issues, contingency planning, configuration management, computer support and operations, incident handling, and IT security awareness and training. Additional information on personnel screening and physical and environmental controls can be found in NPR 1600.1, NASA Security Program Procedural Requirements.

Chapter 15 System Contingency Planning

15.1 Contingency Planning

15.1.1 NASA shall follow the contingency planning guidance in NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.

15.1.2 It is critical that the services provided by NASA's information and technology resources and their associated information infrastructure are able to operate effectively

without excessive interruption.

15.1.3 IT contingency planning refers to the coordinated strategy that involves plans, procedures, and technical measures that enable the recovery of an IT system or systems and the associated operations and data after a disruption in service.

15.1.4 The contingency planning strategy encompasses several different types of contingency plans, each with its own focus. NASA's goal is to use the contingency planning process to prepare response, recovery, and continuity activities to avert disruptions affecting NASA's most critical business processes. Because there is an inherent relationship between an IT system and the business process it supports, there must be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

15.1.5 Contingency planning should be documented at a level appropriate to a coordinated response. To avoid duplication of effort and uncoordinated response, lower-level elements of the response should reference the plan and document only internal contingency measures that are not needed to be visible to interdependent systems.

15.1.6 Although there are many types of contingency plans, each master or subordinate system need only address the subset necessary for that system. Contingency plans shall be incorporated into the SSP.

15.2 Business Impact Analysis

15.2.1 NASA shall:

a. Follow NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, Appendix B, for Business Impact Analysis (BIA).

b. Follow NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, Appendix A, to create each system's contingency plan.

15.2.2 The BIA is considered a key step in the contingency planning process. The BIA enables the information system owner and the information owner to fully characterize the system requirements, processes, and interdependencies and to use this information to determine contingency requirements and priorities for NASA's most critical business processes and the supporting IT services.

15.2.3 The BIA correlates specific system components with the critical services that they provide, and based on that information, characterizes the consequences of a disruption to the system components. Results from the BIA will be appropriately incorporated into the analysis and strategy development efforts for the organization's Contingency Plan, Continuity of Operations Plan, Business Continuation Plan, and Business Resumption Plan.

15.3 Contingency Planning Requirements

15.3.1 NASA contingency planning processes shall:

a. Encompass response, recovery, and continuity activities to avert disruptions affecting NASA's most critical business processes.

b. Ensure that all NASA IT systems have a coordinated contingency strategy that involves plans, procedures, and technical measures that enable the recovery of an IT system or systems and the associated operations and data after a disruption in service.

c. Develop, implement, and annually test contingency plans and procedures that:

(1) Ensure continuity of operations for information systems that support the operations and assets of the Agency consistent with the information systems' risk assessments. This includes notification and activation procedures, recovery operations, and "return to normal" processes.

(2) Meet the needs of the organization and its requirements, including customer expectations.

(3) Provide established procedures to recover a system following a disruption in service.

(4) Can stand alone.

(5) Contain detailed roles, responsibilities, teams, and procedures associated with restoring an IT system following a disruption and would serve as a "user's manual" for executing the recovery strategy to restore normal processing.

(6) Document technical capabilities designed to support contingency operations.

(7) Balance detail with flexibility; usually the more detailed the contingency plan is, the less scalable and versatile the approach.

(8) Call for the review of accounts at least annually.

(9) Appear as a section of the security plan or as a separate document with a copy attached to the plan as an appendix, depending on the size and complexity of the system.

(10) Provide quick and clear direction in the event personnel unfamiliar with the plan or the systems are called on to perform recovery operations that are clear, concise, and easy to implement in an emergency.

(11) Use checklists and step-by-step procedures where possible. A concise and well-formatted plan reduces the likelihood of creating an overly complex or confusing plan.

(12) Address any assumptions made in the contingency plan, such as the assumption that all key NASA personnel would be available in an emergency. However, assumptions should not be used as a substitute for thorough planning. For example, the contingency plan should not assume that disruptions would occur only during business hours; by developing a contingency plan based on such an assumption, the Contingency Planning Coordinator (CPC) might be unable to recover the system effectively if a disruption were to occur during non-business hours. The CPC:

(i) Is typically a functional or resource manager.

(ii) Develops the strategy in cooperation with other functional and resource managers associated with the system or the business processes supported by the system.

(iii) Manages development and execution of the contingency plan.

(iv) Identifies and coordinates with internal and external points of contact (POC) associated with the system to characterize the ways that they depend on or support the IT system, including organizations that provide or receive data from the system, as well as contacts supporting any interconnected systems.

(v) Evaluates the system to link these critical services to system resources.

d Ensure that the guidance provided by NPR 1040.1, NASA Continuity of Operations Planning (COOP) Procedures and Guidelines, is followed for IT systems that are identified as MEI.

15.4 Additional System Contingency Planning References

a. NPR 1040.1, NASA Continuity of Operations Planning (COOP) Procedures and Guidelines.

b. NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

| NODIS Library | Legal Policies(2000s) | Search |

DISTRIBUTION:
NODIS